COMMONWEALTH OF VIRGINIA

Information Technology Resource Management Standard

Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard

Virginia Information Technologies Agency

Preface

Publication Designation

COV ITRM Standard SEC2003-02.1

Subject

Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media

Effective Date

October 29, 2003

Supersedes

No prior Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard

Scheduled Review

One (1) year from effective date

Authority

Code of Virginia, §2.2-2002; §2.2-2003; §2.2-2004; §2.2-2007; §2.2-2010
(Powers and duties of the CIO)

Code of Virginia § 2.2-2651
(Powers and Duties of the Council on Technology Services)

Code of Virginia, §2.2-2005; §2.2-2006
(Powers and duties of the Virginia Information Technologies Agency; "VITA")

Code of Virginia §2.2-3803
(Administration of systems including personal information; Internet privacy policy)

Scope

This standard is applicable to all State agencies, their field operations, and institutions of higher education (collectively referred to as "Agency") that surplus, transfer, trade-in, otherwise dispose of, or replace the computer hard drives and electronic media resources in the Commonwealth. This standard also applies to equipment owned or leased by the agency. The heads of State agencies, the heads of their field offices, and the heads of institutions of higher education are responsible for compliance with this standard. This standard is offered as guidance only to local government entities.

Purpose

1) To define the minimum requirements for the removal of Commonwealth data from an agency's computer hard drives and electronic media resources prior to its being surplused, transferred, traded-in, disposed of, or the hard drive is replaced.
2) To prevent unauthorized use or misuse of state information, and promote the privacy and security of sensitive and/or confidential information resources within the Commonwealth.
3) To foster state agency compliance with federal regulations dealing with the confidentiality of personally identifiable information. Included are regulations such as the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act (aka, Financial Services Modernization Act), and the Family Educational Rights and Privacy Act.

Objectives

- Define and promulgate the minimum requirements for the removal of Commonwealth data from an agency's computer hard drives and electronic media resources prior to its being surplused, transferred, traded-in, disposed of, or the hard drive is replaced.
- Define a process to certify an agency's removal of Commonwealth data from its computer hard drives and electronic media resources.
- Define a process to audit the removal of Commonwealth data from an agency's computer hard drives and electronic media resources.

General Responsibilities

Chief Information Officer
In accordance with the *Code of Virginia*, the Chief Information Officer shall "*Direct the formulation and promulgation of policies, guidelines, standards, and specifications for the purchase, development, and maintenance of information technology for state agencies, including, but not limited to, those (i) required to support state and local government exchange, acquisition, storage, use, sharing, and distribution of geographic or base map data and related technologies, (ii) concerned with the development of electronic transactions including the use of electronic signatures as provided in § 59.1-496, and (iii) necessary to support a unified approach to information technology across the totality of state government, thereby assuring that the citizens and businesses of the Commonwealth receive the greatest possible security, value, and convenience from investments made in technology.*"

Council on Technology Services (COTS)

In accordance with the *Code of Virginia*, the Council on Technology Services is assigned the following duties: "*to advise the Chief Information Officer on the services provided by the Virginia Information Technologies Agency and the development and use of applications in state agencies and public institutions of higher education.*"

Virginia Information Technologies Agency (VITA)
In accordance with the *Code of Virginia*, the Virginia Information Technologies Agency (VITA) is assigned the following duties: "*Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions.*"

All State Agencies
are responsible for complying with COV ITRM policies and standards and considering COV ITRM guidelines issued by the Chief Information Officer.

Definitions

Removal of Commonwealth data: Removal of Commonwealth data from hard drives and electronic media is the process of removing sensitive and/or confidential programs or data files on computer hard drives or electronic media in a manner that gives assurance that the information cannot be recovered by keyboard or laboratory attack.

Related COV ITRM Policies, Standards, and Guidelines

COV ITRM Policy 90-1: Information Technology Security

COV ITRM Standard SEC2001-01.1: Information Technology Security Standard

COV ITRM Guideline SEC2001-01.1: Information Technology Security Guideline

Table of Contents

Background

The surplusing, transfer, trade-in, disposal of computers, or replacement of electronic storage media, and computer software can create information security risks for the agency. This also includes equipment reassigned, or released, or no longer in use in the agency. These risks are related to potential violation of software license agreements, unauthorized release of sensitive and/or confidential information, and unauthorized disclosure of trade secrets, copyrights, and other intellectual property that might be stored on the hard disks and other storage media. It should be noted that all agencies computer hard drives especially those containing sensitive and/or confidential data must have all Commonwealth data securely removed from their hard drives as specified by this policy before a computer system is surplused, transferred, traded-in, otherwise disposed of, or the hard drive is replaced.

Removal of confidential information in the past might have been accomplished by using the FORMAT command or the DOS FDISK command. Ordinarily, using these procedures gave users a sense of confidence that their data had been completely removed. When using the FORMAT command, Windows displays a message such as:

Important: Formatting a disk removes all information from the disk.

The FORMAT utility actually creates new FAT or ROOTS tables, leaving all previous data on the disk untouched. Moreover, an image of the replaced FAT and ROOT tables are stored, so that the UNFORMAT command can be used to restore them. FDISK merely cleans the PARTITION TABLE (located in the drive's first sector) and does not remove anything else.

In recent years advances in data recovery have been made such that data can be reclaimed in many cases from hard drives that have been wiped or cleared. Free and commercial software exist that use techniques such as Partial Response Maximum Likelihood (PRML), Magnetic Force Microscopy (MFM) and other recovery methods based on patterns in erased bands to recover cleared data.

Approach

The heads of State agencies, the heads of their field offices, and the heads of institutions of higher education are responsible for compliance with this standard.

Failure to expunge data that might be exposed under such risk situations could violate federal laws including but not limited to the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), The Family Educational Rights and Privacy Act (FERPA), etc.

This standard also applies to equipment owned or leased by the agency. All hard drives (this includes instances where equipment has multiple hard drives) and electronic storage media shall have all Commonwealth data properly removed prior to disposal or release. Data removal procedures shall be properly documented in accordance with the processes outlined below in sections B, C and D to prevent unauthorized release of sensitive and/or confidential information that may be stored on that equipment and other electronic media. This is to include all computer equipment that has memory such as personal computers, PDAs, routers, firewalls and switches.

Examples of other media include, but are not limited to, tapes, diskettes, CDs, DVDs, worm devices, and USB data storage devices.

Reviews

A full review of the COV ITRM Standard SEC2003-02.1 is anticipated annually.

Statement of ITRM Requirements for the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media

This section groups the specifications of the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard.

A. Removal of Commonwealth Data from Computer Hard Drive and Electronic Media

The following standards must be followed by all agencies as well as their field offices when a computer system is surplused, transferred, traded-in, or disposed of, or the hard drive is replaced. The following standards also apply to contractor-supplied computers.

A.1 Standards

A.1.a) Before a computer system is surplused, transferred, traded-in, disposed of, or the hard drive is replaced, all sensitive and/or confidential program or data files on any storage media must be completely erased or otherwise made unreadable in accordance with this procedure unless there is specific intent to transfer the particular software or data to the purchaser/recipient.

A.1.b) Hard drives of surplus computer equipment must be securely erased within 60 days after replacement.

A.1.c) Whenever licensed software is resident on any computer media being surplused, transferred, traded-in, disposed of, or the hard drive is replaced, the terms of the license agreement must be followed.

A.1.d) After the removal of Commonwealth data from the hard drive is complete, the process must be certified, as specified below, and a record maintained as specified by the agency's records retention schedule.

A.1.e) Each agency head or head of an institution of higher education should create an audit function to randomly test for compliance with this standard any computer hard drives or electronic media that are surplused, ready for public auction, transferred, traded-in, disposed of, or when the hard drive is being replaced.

B. Removal of Commonwealth Data from Hard Drives

The following section outlines the acceptable methods to expunge data from storage media. Removal of Commonwealth data must be performed on hard drives to ensure that information is removed from the hard drive in a matter that gives assurance that the information cannot be recovered. Before the removal process begins, the computer must be disconnected from any network to prevent accidental damage to the network operating system or other files on the network.

There are three acceptable methods to be used for the hard drives:

- Overwriting – Overwriting is an approved method for removal of Commonwealth data from hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented.

- Degaussing – A process whereby the magnetic media are erased, (i.e., returned to a zero state). Degaussing (demagnetizing) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable by keyboard or laboratory attack.

- Physical Destruction – Hard drives should be physically destroyed when they are defective or cannot be economically repaired or Commonwealth data cannot be removed for reuse. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive.

The method used for removal of Commonwealth data, depends upon the operability of the hard drive:

- Operable hard drives that will be reused must be overwritten prior to disposition. If the operable hard drive is to be removed from service completely, it must be physically destroyed or degaussed.

- If the hard drive is inoperable or has reached the end of its useful life, it must be physically destroyed or degaussed.

Clearing data (deleting files) removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is **not** an acceptable method of removing Commonwealth data from agency owned hard disk storage media.

Overwriting

Overwriting is an approved method for the removal of Commonwealth data from hard disk drives. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. All software products and applications used for the overwriting process must meet the following standards:

B.1 Standards

B.1.a) The data must be properly overwritten with a pattern. Department of Defense (DOD standard 5220.22-M) requires overwriting with a pattern, and then its complement, and finally with a random pattern of 1's and 0's.

B.1.b) Removal of Commonwealth data is not complete until three overwrite passes and a verification pass are completed.

B.1.c) The software must have the capability to overwrite the entire hard disk drive, independent of any BIOS or firmware capacity limitation that the system may have, making it impossible to recover any meaningful data.

B.1.d) The software must have the capability to overwrite using a minimum of three cycles of data patterns on all sectors, blocks, tracks, and any unused disk space on the entire hard disk medium.

B.1.e) The software must have a method to verify that all data has been removed.

B.1.f) Sectors not overwritten must be identified.

Degaussing

Degaussing is a process whereby the magnetic media is erased. Hard drives seldom can be used after degaussing. The degaussing method will only be used when the hard drive is inoperable and will not be used for further service.

Please note that extreme care should be used when using degaussers since this equipment can cause extreme damage to nearby telephones, monitors, and other electronic equipment. Also, the use of a degausser does not guarantee that all data on the hard drive will be destroyed. Degaussing efforts will be audited periodically to detect equipment or procedure failures. The following standards must be followed when hard drives are degaussed:

B.2 Standards

B.2.a) Follow the product manufacturer's directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing.

B.2.b) Shielding materials (cabinets, mounting brackets), which may interfere with the degausser's magnetic field, must be removed from the hard drive before degaussing.

B.2.c) Hard disk platters must be in a horizontal direction during the degaussing process.

Physical Destruction

B.3 Standards

B.3.a) Hard drives must be destroyed when they are defective or cannot be repaired or Commonwealth data cannot be removed for reuse.

B.3.b) Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive. This can be attained by removing the hard drive from the cabinet and removing any steel shielding materials and/or mounting brackets and cutting the electrical connection to the hard drive unit. The hard drive should then be subjected to physical force (pounding with a sledge hammer) or extreme temperatures (incineration) that will disfigure, bend, mangle or otherwise mutilate the hard drive so it cannot be reinserted into a functioning computer.

B.3.c) Multiple holes drilled into the hard disk platters is another method of destruction that will preclude use of the hard drive and provide reasonable protection of data written on the drive.

C. Removal of Commonwealth Data from Other Electronic Devices

C.1 Standards

C.1.a) Electronic devices that hold user data or configurations in non-volatile memory shall have all Commonwealth data removed by either the removal of the battery or electricity supporting the non-volatile memory or by such other method recommended by the manufacturer for devices where the battery is not removable. This is to include all computer equipment that has memory such as personal computers, PDAs, routers, firewalls and switches

D. Removal of Commonwealth Data from Other Computer Media

D.1 Standards

D.1.a) If) If there is any risk of disclosure of sensitive data on media other than computer hard drives, that media should be destroyed. Disintegration, incineration, pulverization, shredding or melting are acceptable means of destruction. Examples of other media include, but are not limited to, tapes, diskettes, CDs, DVDs, worm devices, and USB data storage devices.

E. Certification of the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media

Each agency is responsible to audit the removal of Commonwealth data for compliance with this standard when any computer hard drives or electronic media are surplused, transferred, traded-in, disposed of, or the hard drive is being replaced as well as to insure the audit process occurs in a timely manner, and the audit controls are effective.

E.1 Standards

E.1.a) Prior to submitting surplus forms to the agency's appropriate organizational unit, the process for removal of Commonwealth data must be documented on a form that explicitly outlines:

1. The method(s) used to expunge the data from the storage media

2. The type of equipment/media being from which Commonwealth data is removed.

3. The name of the person responsible for the removal of Commonwealth data.

4. The name and signature of their supervisor.

E.1b) The form must be completed and a copy affixed to the hard drive. The completed form must be maintained in a central location designated by the Site Security Officer for audit purposes.

Recommended Software for the Removal of Commonwealth Data from Hard Drives and Electronic Media

According to the manufacturer's claims, the following software meets Department of Defense (DOD) Standard (5220.22-M) for the removal of data from hard drives and are, as examples, suggested for use:

- Active@ KillDisk by L Soft Technologies, Inc. (Free)
- Wiperaser XP by LIVeye, SDC (Shareware)
- Eraser by Heidi Computers, LTD (Free)
- GDISK by Symantex, Inc
- BC-WIPE (shareware) – can be downloaded from www.jetico.com
- BC-WIPE by Tucows, Inc.

Appendix A: Assignment of Uniform Alphanumeric Publication Designations for all Policies, Standards, and Guidelines

The Policy, Practice & Architecture (PP&A) Division of the Virginia Information Technologies Agency (VITA) is responsible for assigning a uniform alphanumeric Publication Designation (PD) to all Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Policies, Standards, and Guidelines (PSG). The PD is derived, in part, from components of the Commonwealth Enterprise Architecture (EA) known as "Infrastructure Domains." The "Infrastructure Domains" and Governance are defined in the Commonwealth EA Glossary. The Governance code is used to identify those PSG that are not uniquely related to a specific infrastructure domain, e.g. "IT Project Management" or "IT Project Oversight."

The following alpha codes will be used to identify each PSG:

Infrastructure Domains + Governance	**Code**
Governance and Transitional Processes	GOV
Platform Architecture	PLA
Database Architecture	DAT
Network Architecture	NET
Security Architecture	SEC
Cost Allocation Architecture	COS
Systems Management Architecture	SYS
Information Architecture	INF
Application Architecture	APP
Middleware Architecture	MID

Publication Designations are constructed as follows:

COV ITRM ("Policy," "Standard," or "Guideline") XXXYYYY-ZZZ

Where: XXX is the assigned Infrastructure Domain + Governance code;
YYYY is the year of initial issue; and
ZZZ is the sequential number assigned to link related PSG.

Example: COV ITRM Standard GOV2000-01.1 is a standard that implements COV ITRM Policy GOV2000-01.1.